

“Virtually Unhackable” DEFCON9:

Securing OpenVMS with System Detective

John Robert Wisniewski, a.k.a. zunderflog@vmsone.com
OpenVMS Ambassador, North Texas
Senior Consultant, Compaq Computer Corporation



THE VMS GREEN TEAM

John Robert Wisniewski, a.k.a. zunderflog@vmsone.com

OpenVMS Ambassador, North Texas

Senior Consultant, Compaq Computer Corporation

John joined DEC in 1987 as a customer SE, and was invited to become an OpenVMS Ambassador in 1989. In 1997 he joined Compaq and is now directly attached to OpenVMS Engineering (since 1999) John is a customer resource for solving complex enterprise problems with OpenVMS. He is also a steering committee member of the Dallas Ft Worth Compaq User's Group and is active in their many projects. John has been a DECUS/Encompass member since 1983 and a regular speaker at Symposia / CETS since the mid 1980's on topics such as OpenVMS, Computer Graphics, Internet, Security, and the Hacker Underground. John speaks fluent VMS, Linux and Windows and if coaxed will lapse into various other dialects from DEC's long history.

Patrick Jankowiak, a.k.a. opcom@vmsone.com

Field Application Engineer, Alcatel Microelectronics

Patrick is a technologist who works with a wide range of electronics hardware from vacuum tube technology to high-end computer systems. He has served as the editor of Quadwords, the DFWCUG's award winning newsletter, since 1994. He made the initial request for the OpenVMS Hobbyist Program and was the first person to be granted an OpenVMS Hobbyist License from Digital/Compaq. He collects and restores classic "Big Iron" computers including 1970's DEC machines and has built a fully equipped laboratory dedicated to this purpose at his home. He also heads up the DFWCUG's Historical Scanning project with the goal of preserving and making freely available on the web, the older DEC manuals and print sets.

Steven E. Smiley, a.k.a. coremac@vmsone.com

Information Technology Analyst, City of Dallas

For the last 14 years, Steven has been a Systems Administrator for local libraries in Texas and Minnesota, running library automation software on various types of Digital VAXen and Alphas. Additional duties include: installing and managing Cisco routers over various WAN connectivity, designing Websites, managing a Windows NT network of more than 800 computers and currently working on Windows2000 Active Directory design for the City of Dallas. He is a member of ENCOMPASS, active member in the DFWCUG and avid VMS Hobbyist, with multiple Digital Alphas in use at home.

DEFCON9

DEFCON is an annual computer underground conference for hackers held in Las Vegas, Nevada. It has been held every summer for the past nine years. Over the course of this time it has grown in size, and attracted people from all over the planet. Hackers attend to meet others into hacking, hang out with old friends, listen to speeches or just hack on the network. Last year's DEFCON attracted over 4,200 people. Making DEFCON the largest hacking convention on the planet.

DEFCON's goal is create an environment where you can hang out with people from all different backgrounds, who are interested in computer security. The event took place at the Alexis Park Resort in Las Vegas, Nevada.

“Capture The Flag” – How the game works

The Capture the Flag contest is designed to emulate real world Internet security scenarios. The goal is for teams to compromise other teams systems and place a file “flag” in the other teams root directory. A point system was determined at the beginning of the contest and the team that accumulates the most points at the end of the contest is the winner.

Teams consisted of groups of administrators and hackers. These two groups are commonly known as “black hats”, the attackers or hackers and the “white hats” or the administrators that run the servers and services. Participants consisted of people with experience ranging from the beginner level to the professional hacker. The contest is limited to a 72 hour time period for teams to place the flags on their competitors systems and score as many points as possible.

Teams were identified by the last three IP addresses of each subnet. These were the target/victim IP addresses. Each team was required to have at least one machine capable of running vmWare that they would leave exposed to the outside environment.

Teams:

Each team was designated by a color. They also received an SSL certificate that allowed them to access the central reporting web site. The five teams that participated were Orange, Green, Black, Red and Blue.

Rules:

- No coercive force or attacking the web server or central routers
- No Denial of Service (DoS) attacks. DoS attacks may cause the judges to disconnect the attackers Ethernet link
- Root partitions must have at least 64K of writeable space

Objective

The purpose of our presence at DEFCON was to demonstrate the industrial strength and competitiveness of OpenVMS to past, present and future generations, as a web and application server and for mission critical operations directly connected to the Internet without a firewall. Our goal was to install an OpenVMS server, running Telnet, FTP, WEB and Personal WEB services and maintain availability and integrity during attacks to any of the previously mentioned services. We also needed to prevent hackers from gaining access to unauthorized files and consequently to avoid hackers from “Capturing the Flag”.

Competitive Environment

DEFCON participants are not representing a particular company. Most contestants participate for the sake of demonstrating their skills and to position themselves as part of the hacker elite. The teams formed from the people who showed up at the DEFCON9 event or had played the game at previous DEFCON events.

Our Team

The Green Team was built (banded together) from system administrators and hackers who had not participated in the game the previous year but who were all well seasoned and mostly in their late 20’s to early 40’s. The other teams were visibly younger in their early 20’s to early 30’s – Everyone had laptops with every conceivable TCP/IP scanning, sniffing and probing tool imaginable from the hacker underground.

Participants hid their real identities and jobs but it was clear to us that the other members of the Green Team were computer professionals of similar backgrounds. We had all come as server administrators to “Play the Game” and test our mettle against the hackers’ onslaught.

Hardware and Software Configuration

The VMS Green Team decided to participate with an Alpha workstation configured as follows:

- 512MB RAM
- 2 fixed drives
- OpenVMS 7.2-1H1
- TCPIP v5.0
- FTP and Telnet
- Apache Web Server

We began building the box in February 2001 and worked on it part time until the event. The system utilized standard distributions of OpenVMS (Alpha) and PointSecure's System Detective product.

Total amount of time invested in the VMS system was about 5 days (about 40 hours work hours) to build, secure, deploy and test, the system and applications for our CTF/DEFCON entry.

It took about 3 iterations to explore, define and test all the security policies we wanted from System Detective.

In order to attract hackers to our site, the team created a Digital Command Language (DCL) script that automatically welcomed all comers and offered a menu of terminal games (Figure 1) or the ability to create a shell account including a user web page for them to modify.

The purpose of the shell account was, in spirit of the CTF rules, to offer real-world services just like any enterprise might have available on their network. The rules also stated that any hacker could request a private account on any server in competition and the administrator was obligated to create one for them. The easiest way to do this was to automate the task from a non-privileged account.

Security was a major issue and to enhance OpenVMS security we selected PointSecure's System Detective AO to help insure the integrity of the server and it's files.

System Detective AO offered some advantages that would allow us to achieve our goals as well as to provide us with audit logs that we could analyze after the convention was over and help us understand hacker behavior and attacks.

We took advantage of some of the System Detective AO features and changed its process and user name so that hackers would not be alerted as to what security software we were utilizing. We then, proceeded to configure System Detective so we could capture every keystroke, login and any other hacking attempts to the system without the hackers' knowledge. Furthermore, we created a security configuration file that would prove unhackable.

Focus on Security

How to lock the system

As mentioned earlier, we decided to utilize PointSecure's System Detective to enhance security for what we considered to be the weak links or back doors to our server. Also, we configured System Detective AO to block the TCP/IP port as if it was a firewall. All configuration of System Detective AO was done through the configuration file that was especially customized for our competition.

What to lock and what not to lock

One of the most important issues when locking the system was to prevent anybody from placing their flags into the root directory "SYSSYSROOT:[000000]". Besides locking the standard system administration files and images such as SYSUAF and Authorize, we disabled common utilities such as VMSInstal, Assign, Rename, Copy, Edit, Create, FTP or any other program that could help the hackers place their flag on our system.

Running stealth

Part of running a successful security system is to not give the intruder any indication that there is a system waiting for the intrusion. By utilizing the change process name and change user name features included in the System Detective AO product, we were able to camouflage the application so it would be more difficult to identify if someone did try to locate and shut down the System Detective application from the "Inside".

What to monitor

To monitor access, we created some rules within System Detective AO's configuration file in which we defined the type of connections that we were going to track and the images that we wanted to trigger notifications in case some non-authorized entity attempted to run them. Most of the items included in the monitoring section were the same as those in the locking section.

Going into the conference we understood the average time to place a file in the root directory, thus we set the idle locking capabilities of System Detective AO on a short timer (2 minutes) and locked intruders keyboards without notifying them of the locking process and without telling them how to unlock the keyboard.

Where Hackers failed

As mentioned earlier, we established a menu (Figure 1) with some game choices to attract visitors. We also gave users the ability to create simple web pages with a non-system account.

```
Record 1 displayed, press a key for next record:
Good afternoon 15-JUL-2001 12:06:14.90

      * Terminal Games from a Simpler Time *

A  BATTLESTAR
B  DOOMSDAY 2000 (Operation Thunderbolt)
C  Hack (Dungeons)
D  Moria 4.81 (Dungeons on Steroids)
E  Star Trek (The Terminal Game c1982... )
F  Dungeon (One of the originals...)
G  ZK (Adventure game that explores DEC's Spitbrook facility 1983)
H
I
J

      2  FINISH WITH THIS MENU

Your choice:
```

Figure 1. Menu designed to attract hackers to our site

In our analysis, we discovered that some hackers tried to explore the system by patching through the accounts established for the games and that did not require passwords and also by trying to hit our TCP/IP and FTP ports. Something that we found out during the contest was that most hackers scanned and tried to hit the high ports. As explained to us by one of PointSecure's system administrators, inexperienced network administrators typically ignore securing high ports and those ports are the major back doors for many real-world environments.

Excerpts from System Detective Report Facility from events captured at DEFCON9:

System Detective Report Facility - PointSecure, Inc.

Report being generated from node SHAGGY at 15-AUG-2001 10:43:15.79

Check for AO PASS

Using default database of openv\$root:[system_detective]detective_database.dat

Scanning the Detective database for selected records...

15-JUL-2001 12:04:28 => Event Severity: INFORM

Username: INTERnet, Process: TCPIP\$INET_ACP, Node: ASTRO

Terminal: DETACHED, Port: *Undefined*, Security Event ID: 102303734410481838

> Event Description: User has had IMAGE TERMINATION due to unauthorized action

> Event Trigger: IMAGE = ACP.EXE

> Event Reason: User INTERnet has executed image ACP.EXE

System Detective detects an illegal request for the Access Control Protocol (ACP) image and terminates the session.

15-JUL-2001 12:05:57 => Event Severity: INFORM

Username: THEWIZ, Process: THEWIZ, Node: ASTRO

Terminal: OPA0:, Port: *Undefined*, Security Event ID: 12783734410481838

> Event Description: User has been MONITORED (RECORDED) due to trigger event

> Event Trigger: IMAGE = TELNET

> Event Reason: User THEWIZ has executed image TELNET

> Session Log File:

OPENV\$ROOT:[SYSTEM_DETECTIVE.LOG]DETECTIVE_11.LOG;1

System Detective initiates monitoring of a Telnet session established by an authorized user at the console level.

15-JUL-2001 12:06:14 => Event Severity: INFORM
Username: DEFCON_GAMES, Process: DEFCON_GAMES, Node: ASTRO
Terminal: TNA10:, Port: Host: 10.255.30.252 Port: 1028, Security Event ID:
3406265610481839
> Event Description: Has logged into the host system
> Session Lock Status: **Session Lock loaded as requested**
> Event Trigger: USERNAME = *
> Event Reason: User DEFCON_GAMES is using OpenVMS username *

System Detective initiates the Session locking mechanism that will eventually terminate any idle process. The locking mechanism is executed, based on configuration parameters, the hacker will not receive any notification of when the system will be locked or how to unlock the keyboard, deceiving him or her into thinking that the computer keyboard “froze” and that rebooting the computer or telnet session was required. In a commercial environment, System Detective will be configured to prompt users about the locking mechanism that took place and the system will allow them to unlock via their personal OpenVMS password.

15-JUL-2001 12:06:16 => Event Severity: INFORM
Username: DEFCON_GAMES, Process: DEFCON_GAMES, Node: ASTRO
Terminal: TNA10:, Port: Host: 10.255.30.252 Port: 1028, Security Event ID:
6016265610481839
> Event Description: User has been MONITORED (RECORDED) due to trigger event
> Event Trigger: TERMINAL = TN
> Event Reason: User DEFCON_GAMES has logged into terminal TN
> Session Log File:
OPENV\$ROOT:[SYSTEM_DETECTIVE.LOG]DETECTIVE_13.LOG;1

15-JUL-2001 12:08:34 => Event Severity: INFORM
Username: **TCPIP\$FTP**, Process: **TCPIP\$FTP**, Node: **ASTRO**
Terminal: NETWORK, Port: *Undefined*, Security Event ID: 143536265610481839
> Event Description: **User has had IMAGE TERMINATION due to unauthorized action**
> Event Trigger: IMAGE = TCPIP
> Event Reason: User TCPIP\$FTP has executed image TCPIP

System Detective identifies an intrusion attempt through the FTP port and stops the session.

```
=====
15-JUL-2001 12:09:41 => Event Severity: INFORM
Username: DEFCON_INFO, Process: DEFCON_INFO, Node: ASTRO
Terminal: TNA11:, Port: Host: 10.255.30.246 Port: 1047, Security Event ID:
210836265610481839
> Event Description: User has been MONITORED (RECORDED) due to trigger event
>   Event Trigger: TERMINAL = TN
>   Event Reason: User DEFCON_INFO has logged into terminal TN
> Session Log File:
OPENV$ROOT:[SYSTEM_DETECTIVE.LOG]DETECTIVE_23.LOG;1
=====
```

```
=====
15-JUL-2001 12:10:10 => Event Severity: INFORM
Username: INTERNET, Process: TCPIP$INET_ACP, Node: ASTRO
Terminal: DETACHED, Port: *Undefined*, Security Event ID: 189890464010481839
> Event Description: User has had IMAGE TERMINATION due to unauthorized action
>   Event Trigger: IMAGE = ACP.EXE
>   Event Reason: User INTERNET has executed image ACP.EXE
=====
```

```
=====
15-JUL-2001 12:27:28 => Event Severity: INFORM
Username: INTERNET, Process: TCPIP$INET_ACP, Node: ASTRO
Terminal: DETACHED, Port: *Undefined*, Security Event ID: 10873923210481841
> Event Description: User has had IMAGE TERMINATION due to unauthorized action
>   Event Trigger: IMAGE = TCPIP
>   Event Reason: User INTERNET has executed image TCPIP
=====
```

REPORT scanned 60 events, selected 60 events, from 5 Detective startups

Total startups: 5	Inactivity events: 0	System Sentry events: 43
User Audit events: 15	Event count: 60	Informative events: 60
Warning events: 0	Critical events: 0	

Total events by System Detective AO trigger:

Detective trigger	Related events
-----	-----
TERMINAL	6
USERNAME	7
IMAGE	38
JOBTYPE	9

System Detective sends a notification message:

```
A  BATTLESTAR
B  DOOMSDAY 2000 (Operation Thunderbolt)
C  Hack (Dungeons)
D  Moria 4.81 (Dungeons on Steroids)
E  Star Trek (The Terminal Game c1982... )
F  Dungeon (One of the originals...)
G  2K (Adventure game that explores DEC's Spitbrook facility 1983)
H
I
J

2  FINISH WITH THIS MENU

Your choice:

Message at 15-JUL-2001 12:06:16.71 to terminal TNA10:=>
THIS MACHINE HAS RESTRICTED ACCESS.  ALL ACTIONS ARE RECORDED...

Your choice:
DETECTIVE EVENT 13 <id: 6016265610481839>=> TERMINAL=TN at
```

Figure 2. System Detective notifies user that all actions will be recorded

Summary

Our Accomplishments:

- After about 52 hours of playing, the DEFCON judges (a.k.a. Goons) placed a note in the Scoreboard file that said that the Green Team's VMS box was "Virtually Unhackable" and that hackers might want to move on to another target. (We spent the last half hour of the contest with not a single attack against our box!)
- OpenVMS Apache web server utilizing System Detective AO proved that web pages served could not be modified.
- The Green Team took Third Place in total points.

At the wrap up session at the end of DEFCON9 the winning team, "The GettoHackers," gave the Green Team "Props" (kudos) because our system "Stayed Up" and our "Root" directory was the only one the hackers were not able to compromise.

The Goons pronounced the VMS system "Cool" because in addition to being unhackable we had the best web content and services on the floor. They also noted that we had continuous service of those applications during the entire event despite all the hacking attempts. So we took away the title of "Cool and Unhackable" for our VMS server.

After the contest was over, we reviewed the logs and System Detective keystroke records of what was attempted. It was obvious that many of the hackers were looking for a quick back door, a simple way in, a mechanical method to breaking in.

It is important to mention that hackers are not criminals. Hackers who break the law are computer criminals. Under the noise of a thousand hacker attacks it is possible that some were looking for system weaknesses they may not exploit today, but will tomorrow. What we've learned should help us prevent future criminal activity.

How do you fight computer criminals? You fight them one system at a time, one application at a time, one intrusion at a time. The most import thing we learned during the 2-½ day contest is that it is your system, network, and security people with the right tools that make the difference in these battles. It's people who deploy security policies, lock down systems, configure security tools to enforce policies and, ultimately, who have to monitor systems for security and intrusions.

OpenVMS and PointSecure are some of the best tools available for deploying secure applications on the Internet.

OpenVMS Background

The technology industry is without any doubt the fastest growing industry in terms of change. We have seen computers transform from room-size to almost microscopic devices with an increased capacity for storage and information processing.

In the mid 1970's, Digital Equipment Corporation, a company headquartered in Massachusetts, developed a 32-bit computer known as the VAX (Virtual Address Extension) that utilized its own operating system, Virtual Memory System (VMS).

At its inception, VMS development had the complete attention of more than 1,000 people who worked on the project. Ascending from a company that started as a component manufacturer, the VAX and VMS were the first computer architecture in which both, hardware and software were designed together.

Through the years, VMS has transformed into a multi-platform operating system and became a strong leader for mission critical operations. Furthermore, cluster computing, invented by Digital, has become a widely accepted alternative method of providing higher system availability and scalability using mainstream computing products than can be provided by a single computer system.

With VMS on VAX, Alpha and soon on Intel's Itanium, the continuation of an enterprise class operating system that runs on industry standard hardware will be an unbeatable combination for years to come.

Security for a Changing World

According to Gartner Group research¹, Winn Schwartau, a computer security expert in St. Petersburg, FL, projects that government and industry face dangerous security problems over the next two years.

Annual global losses from computer break-ins are already approximately **\$1.6 trillion**, Schwartau said, adding that, “The number of computer hacking incidents is more than doubling each year.”

Schwartau said that the fact that many IT professionals don’t take security measures seriously is making matters worse. “They take minimum precautions because it interferes with getting things done, which could backfire when a devastating break-in shuts down all their systems,” he said. “What’s more, they [IT people] avoid security, because it’s hard.”

PointSecure, Inc.

PointSecure provides security solutions that allow organizations to proactively secure their OpenVMS systems. Built on a granular rules-based architecture, we provide flexible yet comprehensive utilities for OpenVMS administrators. These solutions allow for automated enforcement of security policies as well as real-time monitoring of users and sessions.

For more information contact:

PointSecure, Inc.

www.PointSecure.com

info@pointsecure.com

(1) 713.868.1222

¹Weinsten, Bob. “Hot jobs of the future: E-everything, Biotechnology, and Security.” August 15, 2001
<<http://www.techrepublic.com/gartnersuggests.jhtml?id=r00520010815wei01.htm>>